COMMITMENTS IN SIGNATURES

ABSTRACT

The present invention provides methods and apparatus for generating a TCR-commitment having properties differing from the properties of a regular commitment. It provides solutions to the problem of packet authentication for multicast and other scenarios requiring fast, compact digital signature/commitment for E-commerce protocols. It also provides a relatively high level of security guarantees required for packet authentication in a way that can handle multiple independent flows, produces authentication fields of fixed size, works in the fully unreliable setting, does not require any packet delays and has the additional property of being able to withstand and smooth over irregular processor loading and bursty packet output rate. In an embodiment, it uses a hybrid approach consisting of the commiter/signer/bidder creating a certificate for the public key of an efficient k-time signature scheme using a regular signature key. The commiter/signer/bidder then signing up to k messages with the private key corresponding to k-time public key. The time consumed to compute a public key signature is amortized over k signatures.